JOSEPH R. BIDEN, III
ATTORNEY GENERAL

DEPARTMENT OF JUSTICE
820 NORTH FRENCH STREET
WILMINGTON, DELAWARE 19801

CONTACT JASON MILLER
PUBLIC INFORMATION OFFICER
PHONE (302) 577-8949
CELL (302) 893-8939
Jason.Miller@state.de.us

Media Release
January 28, 2011

Attorney General Biden urges Delawareans to protect their identities on Data Privacy Day

Wilmington – Today, in recognition of Data Privacy Day, Attorney General Beau Biden warned Delawareans to protect their personal data by taking steps to encrypt their wireless internet networks.

"Hackers can easily snoop on your internet activity," stated Biden, whose office implemented the Identity Theft Passport which helps victims reclaim their identity and repair their finances. "Consumers should guard their privacy and protect themselves from identity theft by taking some simple precautions, including encrypting their home wireless networks. Identity theft victims spend many hours undoing the thieves' damage. Taking steps to prevent the crime can save a lot of time and money later on."

Last May, Google announced it had been collecting unencrypted payload data, which can include user emails, passwords, and browsing activity, over wireless networks. Google's Street View vehicles, which photograph homes, streets, and other landmarks, also were equipped to capture payload data transmitted over unencrypted networks as those vehicles were driving through neighborhoods. Delaware and other states continue to investigate Google's collection of this data.

Manufacturers often deliver wireless routers with the encryption feature turned off. To turn encryption on, consumers should consult the instructions that accompany their wireless router or visit the manufacturer's website. When selecting a level of encryption, keep in mind that Wi-Fi Protected Access (WPA) encryption is more effective than Wired Equivalent Privacy (WEP) encryption. OnGuard Online, a consortium of federal agencies and technology experts, recommends these steps to secure wireless networks (visit www.onguardonline.gov/topics/wireless-security.aspx for more info):

- **Use anti-virus and anti-spyware software, and a firewall**. Install anti-virus and anti-spyware software, keep them up-to-date, and check to ensure that your firewall is turned on.
- **Turn off identifier broadcasting**. Most wireless routers broadcast a signal to any device in the vicinity announcing their presence. Disable the identifier broadcasting mechanism if your wireless router allows it.
- **Change the default identifier on your router**. The identifier (SSID) for your router is likely to be a default ID assigned by the manufacturer to all hardware of that model. Change your identifier to something only you know, and configure the same ID into your router and computer so they can communicate.
- **Change your router's pre-set administrator password**. Manufacturers assigned routers a default password, which are available to anyone, including hackers. Change it to a unique password of sufficient length and complexity to guard against being cracked.
- **Turn off your wireless network when not in use**. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

- **Don’t assume public “hot spots” are secure**. They’re convenient, but not secure.
- **Be careful about the information you access or send from a public wireless network**. Assume that other people can see anything you see or send over a public wireless network.

Visit the Attorney General’s website at www.attorneygeneral.delaware.gov/consumers/ to learn more about protecting yourself against Identity Theft and services available to victims, including the Identity Theft Passport. Data Privacy Day, recognized on January 28, raises awareness of issues surrounding sensitive information and personal data and draws attention to ways that personal data is collected, used, and stored.

# # #